The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
2/8/2011

SUBJECT:
Multiple vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Office Excel, a spreadsheet application. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will result in a denial-of-service condition.

Please note that there are currently no patches available for these vulnerabilities.

SYSTEMS AFFECTED:

- Microsoft Excel 2002
- Microsoft Excel 2003
- Microsoft Excel 2007
- Microsoft Excel 2010
- Microsoft Office 2003
- Microsoft Office XP

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home Users: High

DESCRIPTION:

Four vulnerabilities have been identified in Microsoft Office Excel that could allow an attacker to take complete control of an affected system. These vulnerabilities can be triggered by opening a specially crafted Excel file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted Excel file as an email attachment. In the web based scenario, a user would have to open the specially crafted Excel file that is hosted on a website. When the user opens the Excel file, the attacker's supplied code will execute.

Details of these vulnerabilities are as follows:

- A remote code execution vulnerability exists because the application uses insufficiently validated user-supplied data to increment an index used in an array.
- A remote code execution vulnerability exists because of the way the application parses an 'Office Art' record. When an error occurs, the application will add an uninitialized reference to a linked list. When handling a Windows message the application will traverse the list causing the application to access the bad link; thus corrupting memory
- A remote code execution vulnerability exists because of a dangling pointer issue. This vulnerability occurs when parsing shape data within the Office Drawing format.
- A remote code execution vulnerability exists because of an invalid object type. This vulnerability occurs when parsing an Office art object to a linked list.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will result in a denial-of-service condition.

Please note that there are currently no patches available for these vulnerabilities.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems as soon as they become available.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/46225/

http://www.securityfocus.com/bid/46226/

http://www.securityfocus.com/bid/46227/

http://www.securityfocus.com/bid/46229/

Zero Day Initiative:

http://www.zerodayinitiative.com/advisories/ZDI-11-040/

http://www.zerodayinitiative.com/advisories/ZDI-11-041

http://www.zerodayinitiative.com/advisories/ZDI-11-042/

http://www.zerodayinitiative.com/advisories/ZDI-11-043/